WE CLAIM:

1. A method for securing lawful intercept related data collected by a switch of a telecommunications service provider and stored in a database associated with the switch, comprising the steps of:

encrypting that portion of the database including the intercept related data; and

preventing another entity outside the telecommunications service provider from decrypting that portion of the database including the intercept related data without authorization from the telecommunications service provider.

2. The method according to claim 1, further comprising the step of creating a logical key at the telecommunications company that allows that portion of the database including the intercept related data to be decrypted.

3. The method according to claim 1, further comprising the step of inserting the logical key into that portion of the database including the intercept related data to be encrypted.

4. The method according to claim 1, further comprising the step of creating the key creates a software key that is used for the encryption of that portion of the database including the intercept related data.

5. The method according to claim 1, further comprising the step of blocking access to display commands that cause that portion of the database including the intercept related data to be displayed by the switch.

6. The method according to claim 1, further comprising the step of sending the data base to a vendor with that portion of the database that is encrypted.

7. The method according to claim 6, further comprising the step of upgrading by the vendor without the need to decrypt or otherwise provide access to the sensitive intercept related data.

8. The method according to claim 1, further comprising the step of storing programming code for controlling the switch in that portion of the database including the intercept related data.

9. The method according to claim 1, further comprising the step of providing protection for the intercept related data in accordance with a lawful intercept legislation.

10. The method according to claim 9, wherein the lawful intercept legislation is CALEA.

11. An apparatus for securing intercepted telecommunications data collected by a telecommunications service provider, comprising:

a database for storing the intercept related data; and

a logical key at the telecommunications company that allows that portion of the database including the intercept related data to be decrypted.

12. The apparatus according to claim 11, further comprising a switch at the telecommunications service provider.

13. The apparatus according to claim 11, wherein the logical key is a software key that used for the encryption of that portion of the database including the intercept related data.

14. The apparatus according to claim 11, further comprising a vendor switch.

15. The apparatus according to claim 14, wherein the vendor switch is programmed to prevent display of commands that cause that portion of the database including the intercept related data to be displayed.

16. The apparatus according to claim 11, wherein the database includes upgradeable control data for controlling the switch.